Activity 5: Security Procedures

Adherence to Forensic Procedures

- Screenshot of “Find My Device” could have shown more information not just the basics.
- The types of USB were not recorded with the size and makes, making it harder for them to be tracked and find what data is lost.
- The Mac Addresses of the Phone and Surface 3 laptop were not recorded to allow for them to be traced and prevented from being used.
- The mac addresses from the wireless mouse and wireless keyboard were not recorded, this would have allowed for the last time they accessed the Wi-Fi to be found giving a clearer indication of when they may have actually been taken and in fact if that had been taken or simply mislaid within the office.
- No specific names were given in regards to the meeting, only that is was with senior management, all peoples present should be listed.

Current Security Protection Measures

The current security measures do not allow for full equipment to be recorded, it appears that not all Mac addresses are recorded therefore not all equipment is trackable.

There is currently no form of “Stock / equipment control” in place, making it harder to spot when equipment is missing. There needs to be locked cabinets possible with power supplies to allow for charging whilst locked away safely, these cabinets should be checked daily and any missing equipment can therefore be highlighted immediately.

The devices with the mac address and user login can record when the device was last used and by whom, therefore accounting for who is responsible to have put the equipment away. All locked away equipment should not give access to general workers instead having the manager in charge of the cabinets with only him having the key to open and lock away the devices.

The procedures do not currently highlight exactly who is responsible for carrying out the procedures other than the team leader when available. However, there are likely to be times when the ways to gather incident reports will require a person with an IT background to perform and therefore the team leader will not always be the person for this.

Document 6

Allowing verbal reports of incidents followed by written reports should be discouraged as by passing information through different people could produce a version of events that is not entirely accurate. If this was to continue to be allowed it would be an idea to recorded the verbal conversation to allow for the person then writing the incident report to refer back to if they have forgotten parts of the incident. Another option could be to record any verbal incident reports given to prevent facts changing or being misinterpreted or changed, this could be done using an interview method.

The security incidents should also include the door logger system, as the security incident may not always include a clear visible forced entry, therefore “Gained Access” should be added to the incidents.

A risk assessment must be outlined to determine what the company think of as “Minor Items” and who these items will be delegated will to. The risk assessment should weigh up the likelihood of occurrence with the impact of loss.

Where possible to prevent data theft of a physical nature all work should be kept regularly backed up to allow for data to be restored, and for devices that do not have a TPM any files stored on them should either be encrypted or placed within an encrypted file, to adhere to both the current Data Protection Act and the General Data Protection Regulation coming into force 25th May 2018.

Policies should be put into place for all staff members highlighting their responsibilities both in general day to day aspects of protecting data and equipment as well as the consequences of any policies being broken including the theft of a USB stick that contains sensitive data, these policies should all be agreed with and signed by all staff members.

All incident reports should highlight and include the types of forensic evidence that need capturing including detailed screenshots, with times, dates, and more detailed information.

To prevent a similar incident happening again there are several steps that could be put into place. These include:

CCTV being added to all areas of the building not just the shops and restaurants, this will both deter thieves as well as record any thefts that do take place. They should be placed outside of the lift and stairwell doors as well as the doors to the office themselves.

Insist that all staff using the NFC cards for access to the rooms, keep their cards within an RFID protected wallet to prevent the card details being copied, it could be highlighted to the general public in the shops and restaurants for their own protection about keeping their bank and credit cards safe using a similar wallet, keeping two cards back to back can also jumble the numbers together making it harder to read the cards or even simply wrapping the cards in aluminium foil to prevent the cards being read. There could be posters made for the public areas highlighting the risk.

For staff within a policy they could add that outside of work hours they don’t keep the NFC badges in their possession. Not only is having their card on their person dangerous for RFID skimming but also for physical pick pockets or if the employee was to lose the card out of the office, on the streets or anywhere else in public this would allow the card to be misused. Doing this within a policy will be a low cost to the company and is technically simple.

The NFC policy could also include that the card is not to be lent by anyone else even another colleague who may be trustworthy, this is necessary to prevent the card being misused by another person and then the evidence pointing towards the card holder instead. The person who’s card it was would have to be accountable unless there was strong evidence to suggest otherwise but this could still involve a disciplinary due to the employees putting the company at risk, as it would the company responsible for loss or data or equipment no the employee.

Another option for the organisation for the use of the NFC cards is that if one is reported stolen or lost, in a similar process to a bank card that id is taking off the system to disallow access so even if found any attempt to use the card after it has been cancelled no access can be given. Instead a new ID number for the person who has reported their card lost or stolen is given to them. This would be more technical and involve the card issuers time but would definitely reduce the chances of loss to the company and therefore would be worth doing.

As stated previously all hardware should be kept out of sight to the public to prevent the chances of being stolen, they should be kept locked in a cabinet that has a power supply to still allow for charging to take place even when not in use. This equipment should be checked daily and therefore any missing equipment would be highlighted quickly. The keys should be kept by only the manager to prevent the likelihood of keys being copied or misplaced.

Again using policies it should be highlighted that the responsibility of the equipment lies with the user and any missing equipment or data would lead to disciplinary actions, this could include dismissal, due to the sensitive nature of the data stored it is particularly important that data is protected as if it is not the company could face large fines under the DPA and GDPR.

As USB's have been taken and the timings of which unknown it could be worth disusing them at all this will prevent them from being misplaced or used to steal data unnoticed easily due to their small size they can be placed in someone's pocket unnoticed. The use of USB's is not needed for this company, files can be accessed via a secure VPN so adding USB is adding a security risk that is not necessary. This can be done via the registry and in the USBSTOR setting the value from3 to 4 to prevent anybody using the USBS that could potentially carry a virus or be used to steal sensitive data from the company.

If the BCTAA continue to use USB they must add passwords to them, and place any files within an encrypted file for added security. BCTAA must also make sure that their antivirus includes USB scanning to prevent any malware being added to their systems when used, this is often not available for free antivirus software and even when available is often required to change the settings as by default the USB scanning is often set to "off".

As highlighted previously I would suggest either not using the first four digits for the floor number and business number, although in this instance the likelihood is skimmer software has been used, by using four of the first numbers for this purpose the general number possibilities is reduces greatly from 10 to the power of 10 possibilities to 6 to the power of 6 possibilities. And therefore if the number is used for other parts of the system including log in, it would be much easier to crack and much quicker. I would suggest either only using the floor number or the business number within the 10 digit number in the middle of it also. Or if both numbers have to be kept again don't have them consecutively and at the beginning of the id as it wouldn't take longer for somebody to spot the pattern that the numbers correlate to an area of the building.

In general the company need to make sure all antivirus software is kept up to date with automatic updates allowed. They need to refer and check on any denied access attempts tot the offices on a regular basis.

For BYOD for staff members they need to record their mac addresses and only allow them devices access to the network using a mac address white list. This can be easily done and is not too technical and would ensure that no other devices are on the company network that haven't been authorised to do so. Added to the policies should be that these BYOD will not be used to take photographs of any sensitive information or shared as this would mean immediate dismissal and the staff member being reported to the police for breaking the Computer Misuse Act.

Extra system checks should be made regarding the door access to ensure that not only the times of day and weekends prevent access but also that public holidays are included in these times.

All devices should have the tracking enabled as well to allow for the locations to be found, as well as all local machine access denied to prevent any attempt of changing permissions to allow for entry to confidential files. Also making sure that the TPM is enabled to devices that have it to protect data on these devices. If unauthorised access is gained they will still not be able to access the data on the device.

Finally all incident report documentation should be kept together in a zip file that is password protected and encrypted or within an encrypted file, the permissions for the file should either be set to read only or so that the file is not visible at all to general employees.

I recommend this is kept for longer than the incident, in case any similar incidents were to occur, this would allow for the details to be compared to possibly highlight another security issue that has net been addressed previously.

Within incident management, if more than one floor has been affected it may be worth having a meeting with the EH managers and comparing the access attempts made on the other floors to help with the investigation process.